Cisco
Private Internet Exchange (PIX)
Firewall 520
Version 4.3(1)

Security Target

Version 1.2

Final
December 1998

Prepared for:

Cisco Systems, Inc.
380 Herndon Parkway
Suite 300
Herndon, VA 20170

Prepared by:

Computer Sciences Corporation
7471 Candlewood Road
Hanover, MD 21076

Table of Contents

List of Tables

Conventions and Terminology

Conventions

The notation, formatting, and conventions used in this Security Target are largely consistent with those used in Version 2 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Only the assignment operation is used in this Security Target.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value].

Recommended changes to security requirements are denoted by **bold text**.

Italicized text is used for both official document titles and text meant to be emphasized more than plain text.

Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

> ***User*** - Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
>
> ***Human user*** - Any person who interacts with the TOE.
>
> ***External IT entity*** - Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
>
> ***Role*** - A predefined set of rules establishing the allowed interactions between a user and the TOE.
>
> ***Identity*** - A representation (e.g., a string) uniquely identifying an authorized user, which can be either the full or abbreviated name of that user or a pseudonym.
>
> ***Authentication data*** - Information used to verify the claimed identity of a user.

In addition to the above general definitions, this Security Target provides the following specialized definitions:

> ***Authorized Administrator*** - A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any

access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Authorized external IT entity – Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Cisco PIX Firewall Version 4.3(1) Security Target

1 SECURITY TARGET INTRODUCTION

1 This introductory section presents *security target (ST)* identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.

1.1 ST and TOE Identification

2 This section provides information needed to identify and control this ST and its Target of Evaluation (TOE), the Cisco Private Internet Exchange (PIX) Firewall 520, Version 4.3(1). This ST targets an Evaluation Assurance Level (EAL) 2 level of assurance.

3 **ST Title:** Cisco Private Internet Exchange (PIX) Firewall 520, Version 4.3(1) Security Target, December 1998

4 **TOE Identification:** Cisco PIX Firewall 520, Version 4.3(1)

5 **CC Identification:** Common Criteria for Information Technology Security Evaluation, Version 2.0, May 1998

6 **PP Identification:** U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.c, Draft, November 1998 (referred to as TFFPP)

7 **ST Evaluation:** U.S. Government, Department of Defense

8 **Keywords:** information flow control, firewall, packet filter, network security, traffic filter, security target

9

1.2 Security Target Overview

10 An ST document provides the basis for the evaluation of an *information technology (IT)* product or system (e.g., TOE). An ST principally defines:

- A set of assumptions about the security aspects of the environment, a list of threats which the product is intended to counter, and any known rules with which the product must comply (in Section 3, Security Environment).

- A set of security objectives and a set of security requirements to address that problem (in Sections 4 and 5, Security Objectives and IT Security Requirements, respectively).

- The IT security functions provided by the TOE which meet that set of requirements (in Section 6, PIX Firewall Summary Specification).

11 The ST for a TOE is a basis for agreement between developers, evaluators, and consumers on the security properties of the TOE and the scope of the evaluation. Because the audience for an ST may include not only evaluators but also developers and "those responsible for managing, marketing, purchasing, installing, configuring, operating, and using the TOE,"[1] this ST minimizes terms of art from the *Common Criteria for Information Technology Security Evaluation* (CC).

12 The structure and contents of this ST comply with the requirements specified in the CC, Part 1, Annex C, and Part 3, Chapter 5.

1.3 Common Criteria Conformance Claims

13 The TOE conforms to the *U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments,* Version 1.c, Draft. It also conforms to Parts 2 and 3 of the CC, Version 2.0.

1.4 Security Target Preparation Methodology

14 An ST, like a Protection Profile (PP), contains sections which address Security Environment, Security Objectives, and IT Security Requirements, as well as Security Objectives Rationale and Security Requirements Rationale sections.

[1] *Common Criteria for Information Technology Security Evaluation* (CC), Part 1, C.1, par. 2.

Under certain conditions, the contents of these sections of the ST may be identical with those of the PP, namely, when the ST:

- Claims compliance with the PP.
- Performs no additional operations[2] on the PP security functional requirements.
- Does not extend the PP by adding security objectives and/or security requirements.

15 Under these conditions, the CC states that "*reference* to the PP is sufficient to define and justify the TOE objectives and requirements. *Restatement* of the PP contents is unnecessary" [italics added].[3]

16 In accordance with this CC statement, the methodology used to develop and present this ST includes the following steps:

- Those TFFPP security objectives and requirements with which the ST claims compliance and for which no additional operations are to be performed are included in the ST by reference to the relevant TFFPP section, not by restatement within the ST.
- If the ST will perform additional operations on TFFPP requirements, the ST restates the requirements and performs the operations.
- If the ST extends the TFFPP by adding security objectives and/or security requirements, the ST states the objectives and/or requirements, makes any needed additions to the Security Environment section, and documents suitable Rationale sections.

17 Under the current evaluation scheme, the first evaluation of a TOE claiming conformance to a draft PP serves the additional function of validating the PP.[4] Upon completion of the first evaluation, the draft PP becomes final and incorporates all resolved Observation Reports (ORs) impacting the PP. Because the TFFPP 1.c is a draft PP, and it is anticipated that the TOE evaluation for this ST will be the first to be completed, this ST states the requirements that are likely to result from the resolution of the outstanding ORs, by the completion of this evaluation. Thus, the ST reflects the anticipated final version of the TFFPP 1.1.

[2] The CC allows controlled tailoring of its security functional requirements, by means of four *operations* (namely, refinement, selection, assignment, and iteration; see CC, Part 2, par. 2.1.4).

[3] CC, Part 1, Annex C, par. C.2.8, b.

[4] Validation does not mean the TFFPP was evaluated against the APE requirements of the CC, Part 3.

2 TOE DESCRIPTION

18 This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Overview of the PIX Firewall System

19 This section presents an overview of the Cisco PIX Firewall 520 Version 4.3(1) to assist potential users in determining whether it meets their needs.

20 The Cisco PIX Firewall 520 Version 4.3(1), known as the TOE, consists of two physically distinct components:

- The PIX Firewall, which controls the flow of Internet Protocol (IP) traffic (datagrams) between network interfaces.
- The NT Workstation, by means of which administrators manage the security of the PIX Firewall.

21 The PIX Firewall, an Intel Pentium II-based computer executing the Cisco PIX Firewall ‘image’, provides a point of defense as well as controlled and audited access to services, both from inside and outside an organization’s private network, by permitting or denying the flow of information transiting the firewall. The firewall provides stateful policy enforcement and other network security functionality.

22 The NT Workstation, a Pentium II-based PC with the Microsoft Windows NT operating system, executing Syslog and TACACS+ servers, provides system and security management. Security management includes the management of audit data.

23 The PIX Firewall and NT Workstation contain vital and benign features. Vital features meet at least one of the functional security requirements identified in Section 5. If a vital feature were removed, then the corresponding functional security requirement(s) would no longer be met. Benign features meet no TFFPP requirements, but add no additional risks. If benign features were excluded from the TOE, the functional security requirements would still be met. Conversely, the presence of benign features will not adversely affect the product’s adherence to the TFFPP functional requirements.

24 No claims are made in this ST regarding Cisco firewall functionality not included in this ST. It is therefore emphasized that *operating the TOE outside its evaluated configuration negates the security claims made in this ST*.

2.2 Scope and Boundaries of the Evaluated Configuration

25 This section provides a general description of the physical and logical scope and boundaries of the TOE.

2.2.1 Physical Scope and Boundary

26 The TOE configuration consists of:

- One PIX Firewall, which controls the flow of IP traffic between network elements.
- One NT Workstation, by means of which administrators manage the security of the PIX Firewall.

27 The TOE's physical boundary includes just these two components. The physical scope of the TOE includes the hardware and software elements identified in Table 1.

Table 1: TOE Component Identification

TOE Components	Hardware/Software Elements
PIX Firewall	PIX520
	PIX Firewall ‘image’ 4.3(1)
NT Workstation	Intel Pentium II 333MHz PC with 64+MB of RAM, 6GB of hard disk, 3.5 floppy drive, keyboard, mouse, serial port, color monitor, power cord, and 10/100mbs Ethernet Network Interface Card with Windows NT 4.0 device driver
	Windows NT 4.0 Workstation with Service Pack 3
	NT Services used by the TOE: • File System • NT Security Subsystem • Event Log Services • NT Registry Services
	PIX Firewall Syslog Server 4.3.1
	TACACS+ 1.0
	Applications: • Microsoft Access 7.0
	Utilities: • logfmt 1.0 • pfssfmt 1.0

2.2.2 Logical Scope and Boundary

28 The TOE provides the following security features:

- **Audit:** the PIX Firewall detects the occurrence of selected events, gathers information concerning them, and sends that information to the NT Workstation where it is stored. The NT Workstation also detects the occurrence of selected events (e.g., security administrator actions), gathers information concerning them, and records it. Audit review is also provided by the NT Workstation.

- **Identification and Authentication (I&A):** both the NT Workstation and the PIX Firewall require administrators to identify and authenticate themselves before they can perform any other actions.
- **Information Flow Control**: the TOE controls the flow of incoming and outgoing IP packets.
- **Security Management:** the NT Workstation provides the console interface to the PIX Firewall for security administration of the PIX Firewall. The NT Workstation also provides security administration functions relating to administrator accounts and audit.

29 Software and hardware features outside the scope of the defined TOE Security Functions (TSF) and thus not evaluated are:

- Cut-Through Proxies
- Failover
- PIX Firewall Manager
- Java and URL Filtering
- Mail Guard
- Network Address Translation (NAT)
- Private-Link
- Setup Wizard
- TFTP Configuration Server
- Virtual Private Networks (Ravlin IPSec Encryption Card)
- Remote Administration (Telnet interface)
- Acceptance of updates for internal data structures (e.g., routing tables) from authorized host
- Windows NT 4.0 features not used by the TOE

2.3 Application Context

30 The PIX Firewall interconnects an organization’s internal and external networks and provides a dedicated Ethernet link to the NT Workstation. The network the TOE protects is referred to as the internal network, and the network to and from which connections are controlled is called the external network. The PIX Firewall forms the boundary between the internal network and the external networks. All traffic between the internal and external networks must flow through the PIX Firewall to maintain security. The external network may be accessible to the Internet and may contain systems that provide services such as HTTP (worldwide

web), FTP, SMTP (electronic mail), and Telnet. The PIX Firewall protects the dedicated link to the NT Workstation by not allowing network traffic originating from the organization's internal or external networks to traverse the link. The NT Workstation has no need to access resources on the external or internal networks. In this way, the NT Workstation and all applications and services therein can be considered a trusted subsystem of the TOE.

2.4 Product Type

31 The PIX Firewall is a stateful packet filtering firewall. A stateful packet filtering firewall controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the firewall's administrator. This header information includes source and destination host (IP) addresses, source and destination port numbers, and transport service application protocol (TSAP). For connection-oriented transport services, the firewall either permits connections and subsequent packets for the connection or denies the connection and subsequent packets associated with the connection. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. In addition to IP header information, traffic filter firewalls use other information, such as the direction (incoming or outgoing) of the packet on a given firewall interface.

3 TOE SECURITY ENVIRONMENT

32 In order to clarify the nature of the security problem, which the TOE is intended to solve, this section describes the following:

- Any *assumptions* about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.
- Any known or assumed *threats* to the assets against which specific protection within the TOE or its environment is required.
- Any *organizational security policy* statements or rules with which the TOE must comply.

33 The TOE is intended to be used in environments where either sensitive but unclassified information is processed or the sensitivity level of information in both the internal and external networks is equivalent.

3.1 Assumptions

34 Three security environment assumptions described in the TFFPP have been modified in this ST. Table 2 states these assumptions. These assumptions refine the general assumptions stated in the PP and are applicable to the architecture of this specific TOE.

Table 2: Modified Assumptions and Additions to the PP

Name	Description
A.PHYSEC	The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.
A.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
A.DIRECT	The TOE and associated direct-attached console are available to authorized administrators only.

35 Except for the assumptions named the same as those in Table 2, the TOE claims the assumptions about the security environment described in the TFFPP.

3.2 Threats

36 Threats may be addressed either by the TOE or by its intended environment (for example, using personnel, physical, or administrative safeguards). These two classes of threats are discussed separately.

3.2.1 Threats Addressed by the TOE

37 The TOE addresses the following TFFPP, Section 3.2.1 Threats: T.NOAUTH, T.REPLAY, T.ASPOOF, T.MEDIAT, T.OLDINF, T.AUDACC, T.SELPRO, and T.AUDFUL.

3.2.2 Threats Addressed by the Operating Environment

38 The TOE Operating Environment addresses the same TFFPP, Section 3.2.2 Threats.

3.3 Organizational Security Policies

39 The TFFPP does not identify any organizational security policies with which a traffic-filter firewall must comply. That is, the TFFPP fully characterizes the security problem by means of threats and assumptions alone. This holds, too, for this ST; accordingly, no organizational security policies are here specified.

4 SECURITY OBJECTIVES

40 "The security objectives are a concise statement of the intended response to the security problem."[5] These objectives indicate, at a high level, how the security problem, as characterized in the "Security Environment" section of the ST, is to be addressed.

41 Just as some threats are to be addressed by the TOE and others by its intended environment, so some security objectives are for the TOE and others are for its environment. These two classes of security objectives are discussed separately.

4.1 Security Objectives for the TOE

42 The security objectives for the TOE are the following TFFPP, Section 4.1 Security Objectives: O.IDAUTH, O.MEDIAT, O.SECSTA, O.SELPRO, O.AUDREC, O.ACCOUN, and O.SECFUN.

4.2 Security Objectives for the Environment

43 The security objectives for the TOE environment are those specified in TFFPP, Section 4.2 and in Table 3.

Table 3: Additional Security Objectives

Name	Description
O.PHYSEC	The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.
O.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
O.DIRECT	The TOE and associated direct-attached console are available to authorized administrators only.

[5] CC, Part 3, par. 5.4.

5 IT SECURITY REQUIREMENTS

44 IT security requirements include:

- TOE security requirements and (optionally)
- Security requirements for the TOE's IT environment (that is, for hardware, software, or firmware external to the TOE and upon which satisfaction of the TOE's security objectives depends).

45 These requirements are discussed separately below.

5.1 TOE Security Requirements

46 The CC divides security requirements into two categories:

- *Security functional requirements (SFRs)*, that is, requirements for security functions such as information flow control, audit, identification and authentication.
- *Security assurance requirements (SARs)*, provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, vulnerability assessment).

47 This section presents the security functional and assurance requirements for the TOE.

5.1.1 TOE Security Functional Requirements

48 This section presents the SFRs for the TOE. In accordance with the methodology described in Section 1.4, Security Target Preparation Methodology, this section has the following four subsections:

- *Referenced PP SFRs*: those PP security functional requirements with which the ST claims compliance[6] and for which no additional operations are to be performed. These PP SFRs are included in the ST by reference.

- *Tailored PP SFRs*: those PP security functional requirements with which the ST claims compliance but for which additional operations are to be performed.

- *Additions to PP SFRs* (optional): any security functional requirements additional to those of the PP.

- *SFRs With Strength of Function (SOF) Declarations:* any security functional requirement that requires a SOF declaration.

5.1.1.1 Referenced PP SFRs

49 The TOE shall satisfy the SFRs specified in Table 4. Table 4 lists the CC names of the SFR *components*[7] contained in the TFFPP. For the reader's convenience, the components are grouped by well-known security requirement type (i.e., what is variously called security service, security mechanism, class or family of security requirement, etc.). The types are named in the shaded rows (beginning with "Audit").

[6] Compliance is based on incorporation of the changes recommended in ORs against the TFFPP.

[7] In CC parlance, a *component* is "the smallest set of selectable [requirements] elements that may be included in a PP" or an ST (CC, Part 1, 2.3). An element is "An indivisible security requirement" (*ibid*.).

Table 4: Referenced PP SFRs

Functional Components for the TOE	
Audit	
FAU_GEN.1	Audit data generation
FPT_STM.1	Reliable time stamps
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
Identification and Authentication (I&A)	
FIA_UID.2	User identification before any action
FIA_UAU.1	Timing of authentication
FIA_ATD.1	User attribute definition
Information Flow Control	
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FMT_MSA.3	Static attribute initialization
FDP_RIP.2	Full residual information protection
Security Management	
FMT_SMR.1	Security roles
FMT_MOF.1	Management of security functions behavior
Protection of Security Functions	
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation

50 The TFFPP specifies that some functional requirements are optional and may be omitted from compliant TOEs. Table 5 identifies the SFRs that have been omitted from this ST because the evaluated configuration of Cisco PIX Firewall 520, Version 4.3(1) does not support either Remote Administration of the TOE or updates of TOE information by Authorized External IT Entities.

Table 5: Functional Components Omitted from the TOE

Reference	Description
FIA_AFL.1	Authentication failure handling
FIA_UAU.4	Single-use authentication mechanisms
FCS_COP.1	Cryptographic operation

5.1.1.2 Tailored PP SFRs

51 The TFFPP identifies several SFRs that contain operations to be completed in PP-compliant security targets. This section identifies those TFFPP requirements and performs the required operations. The TOE shall satisfy the resultant requirements.

52 Table 6 names the SFRs for which the ST is required to perform operations. The table also identifies the operations (assignment, iteration, refinement, and selection) performed on them in this ST. Following the table, the individual functional requirements are restated from the TFFPP, and the operations completed.[8]

Table 6: Tailored PP SFRs

SFR ID	Component Name	Operation
Information Flow Control		
FDP_IFF. 1	Simple security attributes	Assignment
Identification and Authentication		
FIA_ATD.1	User attribute definition	Assignment
Security Management		
FMT_MOF.1	Management of security functions behavior	Assignment

FIA_ATD.1 User attribute definition

53 FIA_ATD.1.1 - The TSF shall maintain the following list of security attributes belonging to individual users:

a) identity

b) association of a human user with the authorized administrator role

c) [no additional user attributes]].

FDP_IFF.1 Simple security attributes

54 FDP_IFF.1.1 - The TSF shall enforce the UNAUTHENTICATED SFP based on at least the following types of subject and information security attributes:

a) subject security attributes
   - presumed address

[8] For ease of reading, the bolding, underlining, italics, and bracketing which the PP uses to identify the operations it performs have been removed in the restatement of the requirements below. Only the operations performed by the ST are identified here.

- [no additional subject security attributes]

b) information security attributes

- presumed address of source subject
- presumed address of destination subject
- transport layer protocol
- TOE interface on which traffic arrives and departs
- service
- [no additional information security attributes]

FMT_MOF.1 Management of security functions behavior

55 FMT_MOF.1.1 - The TSF shall provide and restrict the ability to perform the following functions, to an authorized administrator:

a) start-up and shutdown

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows

c) create, delete, modify, and view user attribute values defined in FIA_ATD.1

d) enable and disable single-use authentication mechanisms in FIA_UAU.4 (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network)

e) modify and set the threshold for the number of permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network)

f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network)

g) enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities)

h) modify and set the time and date

i) archive, create, delete, empty, and review the audit trail

j) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools

k) recover to the state following the last backup

l) additionally, if the TSF supports remote administration from either an internal or external network:

- enable and disable remote administration from internal and external networks
- restrict addresses from which remote administration can be performed

m) no additional operations

5.1.1.3 Additions to PP SFRs

56 The ST has no additional requirements beyond those already stated in the TFFPP.

5.1.1.4 SFRs With SOF Declarations

57 FIA_UAU.1 The TOE shall demonstrate that the probability of authentication data being guessed will be less than one in a million.

5.1.2 TOE Security Assurance Requirements

58 The PIX Firewall shall satisfy the security assurance requirements for EAL2, as required by the TFFPP, Section 5.1.2, and defined in Part 3 of the CC.

59 This ST does not augment EAL2 with other security assurance requirements from Part 3 of the CC; nor does it extend EAL2 by explicitly stating additional security assurance requirements not taken from Part 3 of the CC.

60 Table 7 identifies the security assurance requirements components included in EAL2.

Table 7: Referenced PP EAL2 SARs

Reference	Description
ACM_CAP. 2	Configuration items
ADO_DEL. 1	Delivery procedures
ADO_IGS. 1	Installation, generation, and startup procedures
ADV_FSP. 1	Informal functional specification
ADV_HLD. 1	Descriptive high-level design
ADV_RCR. 1	Informal correspondence demonstration
AGD_ADM. 1	Administrator guidance
AGD_USR. 1	User guidance
ATE_COV. 1	Evidence of coverage

Reference	Description
ATE_FUN. 1	Functional testing
ATE_IND. 2	Independent testing - sample
AVA_SOF. 1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

5.2 Security Requirements for the IT Environment

61 The TOE has no security requirements allocated to its IT environment.

6 PIX FIREWALL SUMMARY SPECIFICATION

62 This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

63 This section presents the security functions performed by the TOE and provides a mapping between the identified security functions and the Security Functional Requirements that it must satisfy.

6.1.1 PIX Firewall Security Functions

6.1.1.1 Security Administration [PIA_ADMIN]

64 The NT Workstation provides the only method to modify the TOE configuration by changing parameters on the Syslog Server or the TACACS+ server or via a console login to the PIX Firewall. Only an authorized administrator working through the NT Workstation can perform security management functions. The only authorized users working through the NT Workstation are the authorized administrators. Authorized administrators have full administrative privileges for the TOE. The authorized administrators are assigned the NT role “administrator”. The administrative role is preserved when the administrator logs into the PIX Firewall via TACACS+ protocols query of the NT Security Subsystem.

65 Security attributes belonging to authorized administrators are maintained in the NT Security Subsystem. The User Manager manipulates the properties for each account on the NT Workstation. Using the User Manager, the TOE can maintain identity, authentication data, and a method of associating a human with the authorized administrator role for human users.

66 The administrative functions below require successful login to the NT Workstation and, in some cases, a login to the PIX Firewall. Table 8 below describes the administrative functions and how they are implemented.

Table 8: Security Administration Functions and Implementation Description

Function	Implementation

Table 8: Security Administration Functions and Implementation Description

Startup and shutdown	NT Workstation startup and shutdown commands. PIX Firewall power switch, reset button, and *reload* command.
Create, delete, modify, and view information flow security policy rules that permit or deny information flows	The PIX Firewall controls information flows using the Adaptive Security Algorithm as well as *conduit*, *static*, *outbound*, and *apply* commands.
Create, delete, modify, and view user attributes	NT provides this capability with the User Manager mechanism of the NT Security Subsystem.
Modify and set the time and date	Both the PIX Firewall and the NT Workstation maintain their own clocks. To modify the PIX Firewall, the command *clock set* is used in enable mode. To modify the NT clock, the Date and Time applet in the Control Panel is used.
Archive, create, delete, review, and empty the audit trail	The Audit trail is maintained on the NT Workstation in the Event Log and the Syslog log files. The Event Log is reviewed using Event Viewer and the Syslog logs are files reformatted and imported into Microsoft Access for review. All syslog audit files are stored on the NT Workstation's disk and are protected and audited via NTFS. Creation of the audit trails is performed by the applications.
Backup and recover, where the backup capability shall be supported by automated tools	Backup and recovery is a function of the native utilities on both the NT Workstation and the PIX Firewall.

6.1.1.2 Identification and Authentication [PIA_INA]

67 To gain logical access to any component of the TOE for administrative purposes, the authorized administrators must identify and authenticate via the NT login window and again at the PIX Firewall prompt. Identification and authentication services are performed by the NT Security Subsystem.

68 All passwords generated for use in the TOE environment must follow these rules:

- Minimum of 8 characters
- The possible characters are a-z, A-Z, 0-9 and !@#$%^&*()_+
- The passwords must be changed every 12 months

69 If these rules are followed, the probability of guessing the password is less than one in one million, satisfying the TFFPP strength of function requirement.

70 The only human users that the TOE recognizes are administrators. They have to authenticate themselves to the NT Workstation before they can take any TSF-mediated actions. External IT entities are identified by IP address and PIX Firewall interface (inside, outside) that the IP address is identified on. This IP address is validated against the Adaptive Security Algorithm (ASA) and the PIX Firewall configuration rules, before any flows through the PIX Firewall are established.

6.1.1.3 Information Flow Control [PIA_FLOW]

71 The PIA_FLOW is supported by the ASA and the *conduit*, *static*, *outbound,* and *apply* commands. The header of each TCP/IP packet contains the information used to ensure that a packet reaches its ultimate destination. This same data is used to enforce the UNAUTHENTICATED_SFP. The policy is enforced by the ASA on a packet-by-packet basis, based on the PIX Firewall interface, network layer source and destination addresses, the transport layer protocol (TCP or UDP), and the transport layer destination address, and services. Services are identified by well-known port numbers at the transport layer.

72 The *outbound* and *apply* configuration commands can be used to control access to external resources from internal hosts, based on the following security attributes: internal subject's IP address, the external object's IP address, the transport layer protocol, and the service requested (port number). The keywords *permit* and *deny* can be specified to grant or deny access.

73 Conduits allow limited access to internal networks from external networks, through the TOE, based on the following security attributes: destination IP address, transport protocol, destination port number (in the case of TCP or UDP) and source IP address (or IP address range).

74 Unless a conduit is explicitly created by an authorized administrator, the TOE rejects all requests for services by external, unprotected networks. The TOE will also forward packets requesting access or services from the external to internal interface which comply with a conduit that has been pre-established by the administrator. Unless the administrator configured the firewall to specifically

accept requests from the addresses mentioned in the requirement, the TOE will successfully reject any such request.

75 Enforcement functions for packet flow through the TOE are based on the ASA and the *conduit*, *static*, *outbound,* and *apply* commands. All packet flows through the TOE are received by a network interface card, mediated by the ASA, must satisfy the following rules, before being delivered to the destination network interface card.

76 The conduit command establishes rules that are enforced by the ASA during enforcement of its basic rule set.

77 The ASA basic rules are as follows:

- Allow any TCP connection that originates from the inside network.
- Permit TCP packets from the outside network that are return packets for an existing outgoing connection.
- Drop and log attempts to initiate TCP or UDP connections from the outside network to any IP address for an existing connection.
- Drop and log source routed IP packets from the outside network that is sent to any IP address for an existing connection.
- Silently drop ping requests to IP addresses for an existing dynamic connection.
- Answer, by the PIX Firewall, ping requests directed to static connections.
- Allow any UDP connection that originates from the inside network.
- Drop and log all other packets received on the outside interface.
- UDP connection objects are timed out based on a configurable scheduling frequency timer, started when the connection object is created.
- TCP connection objects are timed out based on a configurable millisecond clock timer, started when the connection object is created.
- Drops packets that arrive on the outside interface with a source IP address on the inside network.

78 The PIX Firewall Network Address Translation (NAT) capabilities have been disabled and are not part of the TOE. The default configuration of the PIX Firewall will reject all traffic destined for a private network.

79 The PIX Firewall ASA algorithm blocks all packets containing loopback addresses and broadcast addresses.

80

81 The operation of the basic rules of ASA can be modified using *conduit, static, outbound,* and *apply* commands

82 The ASA will not permit traffic that arrives on an outside interface with a source IP address on the inside network to flow through the TOE. Similarly, the TOE will prevent traffic that arrives on an inside interface with a source IP address on the outside networks if the *sysopt connection.enforsesubnet* option is enabled.

83 At any given time after the PIX Firewall has been initialized, it will have the following:

- sessions currently going through it
- sessions that had gone through it but have been terminated
- at various times, new sessions initiated

84 The TOE creates flows (sessions) between subjects. Each of the sessions is composed of packets. The packets have mutable fields, immutable fields, and the data payload. The PIX Firewall maintains state of each of the current sessions based upon the mutable and immutable fields of the packet but never retains any information found in the data payload.

85 Current sessions cannot gain access to the state information, mutable and immutable field information, or data payload of any other packet that has passed through the PIX Firewall. Since the PIX Firewall is the single point between the trusted and untrusted networks and since networks work on the basis of one packet on the wire at any time, the PIX Firewall is only dealing with one packet at any time for the inbound and for the outbound queues. These two queues are kept separate, and no interaction is possible. When a new packet is received, it overwrites any memory that had been allocated to a prior packet. The end of the packet is noted as a mutable field of the packet, and the PIX Firewall will not release any memory beyond that end of packet when the packet is sent to the send queue.

86 Mutable fields of the packet are as follows:

- Source and Destination IP address
- Source and Destination TCP/UDP port numbers
- Time to Live
- IP and TCP Checksums
- TCP Sequence and Acknowledgment Numbers

87 All other fields of the IP, TCP, and UDP headers are regarded as immutable, and the PIX Firewall will not change them.

88 Mutable field information is erased from memory when the XLATE timer expires for a given XLATE table entry.

6.1.1.4 Default Configuration [PIA_DEFCFG[9]]

89 Data is not permitted to flow through the TOE after initial connection of power and network connections and when the Installation, Generation, and Startup (IGS) are complete. This provides the most restrictive default values for data flow through the TOE. Using the *conduit*/*apply* commands, the administrator can modify the initial configuration to allow traffic to flow through the TOE.

90 After Installation, Generation, and Startup are completed, the configuration is saved to non-volatile memory and will be invoked on subsequent system startup.

6.1.1.5 Isolation [PIA_SEP]

91 The TOE does not permit untrusted subjects to execute on the TOE itself, thus the security domain maintained by the TSF is the TOE. The TOE only stores and executes security–relevant applications and only stores data required for its secure operation. In addition, the TOE is assumed to be located within controlled access facilities that mitigate unauthorized, physical access.

92 The TOE scope of control is defined as the following: connections between subjects mediated by the TSF such that each connection is a separate domain. Access through the TOE is only permitted based on security policy enforced by the PIX Firewall configuration defined by an authorized administrator. Subjects are uniquely identified by the PIX Firewall by using PIX interface, source IP address, destination IP address, port, and sequence numbers. Using the connection information, the ASA maintains domain separation.

93 There are two objects maintained by the TOE to support connections between hosts. They are the CONNECTION entry and the XLATE entry.

94 CONNECTION entries maintain all information needed to manage a connection (or session) between two hosts. After the ASA determines that a requested connection between two hosts satisfies the security policy established by the PIX firewall administrator, a CONNECTION entry is allocated to manage that connection. When a connection between two hosts is terminated the associated CONNECTION entry is deallocated and returned to the pool of available resources.

95 XLATE entries maintain information about the association between two distinct hosts that have active connections through the PIX. An XLATE entry is allocated

[9] This configuration has been developed to meet the TFFPP requirements and is not recommended by Cisco for all environments.

when a new connection is established between two hosts, and no other connections between them exist. The CONNECTION entries associated with subsequent connections between a distinct pair of hosts are linked to their XLATE entry. When the last connection between two hosts is terminated (and the associated CONNECTION entry is deallocated), the XLATE entry associating those two hosts is deallocated.

6.1.1.6 Audit [PIA_AUDIT]

96 The TOE relies on two audit mechanisms to capture all the audit data required: NT Event Log and PIX Firewall Syslog Server (PFSS). Audit data is generated by the TACACS+ server, the PFSS, and the PIX Firewall. Windows NT and TACACS+ server write audit data using the NT Operating System’s Event Log service. PFSS and the PIX Firewall write their audit data using the PFSS.

97 All auditable events on the PIX Firewall are delivered to the NT Workstation PFSS using a TCP-based Syslog application. This guarantees delivery of the audit messages between the PIX Firewall and the NT Workstation.

98 The PFSS generates two types of log files. The first type is the daily log (Monday.log, Tuesday.log, etc.) containing all the Syslog messages generated during that day from the PIX Firewall. The PFSS also generates a status log (pfss.log) that contains messages related to the operation of the PFSS.

99 The NT Event Log service records events in the following three kinds of logs:

- The system log contains events logged by the NT Workstation system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log.
- The security log can contain valid and invalid logon attempts as well as events related to resource use, such as creating, opening, or deleting either files or other objects.
- The application log contains events logged by applications. All audit messages from the TACACS+ server are written to this log.

100 Both the PIX Firewall and the NT Workstation use their respective PC clocks on their motherboards to generate timestamps for audit records. The NT Workstation uses the Date and Time Control Panel applet to modify the clock, and the PIX Firewall uses the *clock set* command.

101 ***Audit Data Generation***

102 The TOE is able to generate an audit record for each of the auditable events in Table 9. The TOE records, in the log message, the date and time of the event, type of event, subject identity, and outcome (success or failure) of the event.

Table 9: Audit Event Generation

Audit Event	Generated by
Startup of Event Log	The NT Event Log is active on the NT Workstation at all times unless disabled at startup.
Startup and Shutdown of PFSS	The PFSS captures its startup in the pfss.log.
Modifications to the group of users that are part of the authorized administrator role	The User Manager of the NT Security Subsystem generated events when modifications to administrator roles are made.
All use of the user identification mechanism, including the user identity provided	The user identification mechanism is the NT security subsystem. The NT security subsystem records all usage in the Event Log.
All use of the authentication mechanism	The user authentication mechanism is the NT security subsystem. The NT security subsystem records all usage in the Event Log.
All decisions on request for information flow	The PIX Firewall sends Syslog messages auditing all decisions for information flow.
Startup and shutdown of the TOE	The PIX sends a Syslog message when it powers up. The NT Workstation logs startup events.
Create, delete, modify, and view information flow security policy rules that permit or deny information flows	The PIX Firewall sends a Syslog message upon each modification to the PIX configuration. This will include conduit, static, outbound, and apply commands.
Create, delete, modify, and view user attributes	NT Event Log captures the creation of accounts and attributes.
Modify and set the time and date	The PIX Firewall generates a Syslog message when the clock command is issued. The NT Workstation captures the event with Event Log.
Archive, create, delete, review, and empty the audit trail	The NT Workstation generates an audit event when the Event log is cleared. All access to the files generated by the PFSS is audited by the NTFS Security functions.
Backup and recovery, where the backup capability shall be supported by automated tools	All back up and recovery of the audit trail data is done using the NTFS. The backup and recovery commands of the PIX Firewall are logged to the PFSS.

103 *Audit Review*

104 The audit data is presented in human-readable form in both the Event Log and the PIX Firewall Syslog Server logs. The authorized administrator is the only user allowed on the NT Workstation and therefore is the only user who has access to the audit trail. The Event Viewer is a graphical tool used to search the Event Log

and provides the ability to search and sort based on event type and on date and time.

105 To search and sort the logs generated by the PFSS, the logs must be converted to a Microsoft Access database. This is accomplished using the pfssfmt and the logfmt utilities to reformat the pfss.log and daily logs, respectively, into a comma-separated value file. That file is imported into Microsoft Access. Microsoft Access provides the searching and sorting on IP addresses, dates, and times using Access embedded functions.

106 *Audit Storage*

107 The audit trail (event log and Syslog files) is protected by the NT workstation. The NT Workstation uses Microsoft's secure files system, NTFS. At user logon NT generates an access token for the user. The win32 subsystem uses that token to determine the user's access to all files on the NTFS disk. If the user does not belong to a group that has permission to access a file then NTFS denies the user access. All the syslog files are protected by NTFS. Only users belonging to the Administrator group can access and manipulate the audit files. The only users allowed on the NT workstation are the authorized administrators, and authorized administrators are the only users that can modify, archive, and delete audit records.

108 The TOE is able to detect modifications to the audit trail by enabling file operation audit through the NTFS. The following success or failure of the following actions is audited: read, write, execute, delete, change permissions, take ownership.

109 If the audit trail reaches the threshold as defined by the authorized administrator, no new flows through the PIX Firewall will be allowed. Only actions taken by the authorized administrator are permitted and logged until disk space is available. The thresholds are based on percentage of disk space. If the proper threshold is set by the administrator, no audit data will be lost.

6.1.2 Mapping of TOE Security Functions to Functional Requirements

110 Table 10 describes the mapping between the functional capabilities of the PIX Firewall and the SFRs specified in the PP. For completeness, the table (within the grayed out columns) identifies those SFRs that are not applicable to the TOE..

Table 10: Mapping Between SFRs and Security Functions

Security Functions	Functional Security Requirements																			
	FMT_SMR.1	FIA_ATD.1	FIA_UID.2	FIA-AFL.1	FIA_UAU.1	FIA_UAU.4	FDP_IFC.1	FDP_IFF.1	FMT_MSA.3	FDP_RIP.2	FCS_COP.1	FPT_RVM.1	FPT_SEP.1	FPT_SMT.1	FAU_GEN.1	FAU_SAR.1	FAU_SAR.3	FAU_STG.1	FAU_STG.4	FMT_MOF.1
PIA_ADMIN	x	x		▨		▨					▨									x
PIA_INA			x	▨	x	▨					▨									
PIA_FLOW				▨		▨	x	x		x	▨	x								
PIA_DEFCFG				▨		▨			x		▨									
PIA_SEP				▨		▨					▨		x							
PIA_AUDIT				▨		▨					▨			x	x	x	x	x	x	

6.2 Assurance Measures

111 The TOE satisfies the SARs specified in the TFFPP. This section identifies the Configuration Management, System Delivery Procedures, System Development Procedures, Guidance Documents, Testing, and Vulnerability Analysis measures applied by Cisco to satisfy the CC EAL2 assurance requirements summarized in Table 7.

6.2.1 Configuration Management

112 The Configuration Management measures applied by Cisco include assigning a unique product identifier for each release of the TOE. Associated with this Product Identifier is a list of Hardware and Software configuration items that compose a single instance of the TOE. These configuration management measures are documented within the following Cisco documents:

- Configuration Management and Delivery Document, Version 1.0
- Hardware Functional Specification (Lego), Revision 1.2

6.2.2 Delivery and Operation

113 Cisco provides Delivery and Operation documentation that describes what components are delivered with the PIX Firewall, guidance for initially installing it, and warnings about the importance of properly unpacking, installing, and configuring the TOE. These delivery and operation measures are documented within the following Cisco documents:

- Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper, Version 1.0
- Configuration Management and Delivery Document, Version 1.0

6.2.3 Development

114 The Development documents provided by Cisco satisfy the CC functional specification and high-level design development requirements, as well as provide a correspondence between that information and this ST. These architecture measures are documented within the following Cisco documents:

- NT Workstation Architecture document, Version 1.0
- PIX V4.3.1 Architecture and Detailed Design, Version 1.2
- PIX Firewall Syslog Server Document, Version 2.0
- System Log Messages for the PIX Firewall, Version 4.2
- Cisco PIX Firewall 520 Version 4.3(1) Correspondence White Paper, Version 1.0
- Cisco PIX Firewall 520 Version 4.3(1) Administrative Guidance White Paper, Version 1.0
- Hardware Functional Specification (Lego), Revision 1.2
- Configuration Guide for the PIX 4.2
- PIX Firewall Quick Installation Guide 4.2

6.2.4 Guidance

115 The Guidance Documents provided by Cisco include both Installation and Configuration manuals that guide administrators through the process of unpacking, installing, and configuring the PIX Firewall. These documents also warn the

administrator about common mistakes that could lead to an insecure configuration. These guidance measures are documented within the following Cisco documents:

- Cisco PIX Firewall 520 Version 4.3(1) Administrative Guidance White Paper, Version 1.0
- Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration White Paper, Version 1.0
- Release Notes for the PIX Firewall 4.2
- Configuration Guide for the PIX 4.2
- PIX Firewall Quick Installation Guide 4.2

6.2.5 Test

116 Cisco performs extensive Testing of the PIX Firewall. The testing performed includes both functional and penetration testing to ensure that the PIX Firewall meets its design goals.

- Cisco PIX Target of Evaluation Test Procedures Document, Version 1.0

6.2.6 Vulnerability Analysis

117 As part of the design and testing process, Cisco performs Vulnerability Analysis of the PIX Firewall. The goal of this analysis is to identify any obvious weaknesses that could be exploited by an attack. The vulnerability analysis is documented within the following Cisco document:

- TTAP PIX Firewall Vulnerability Assessment, Version 1.0

6.2.7 Strength of Function Analysis

118 The Strength of Function Analysis performed on user passwords is provided within the following Cisco document:

- Cisco PIX Firewall 520 Version 4.3(1) Administrative Guidance White Paper, Version 1.0

6.2.8 Mapping of Assurance Measures to Assurance Requirements

119 Table 11 describes the mapping between the assurance measures of the TOE and the SARs specified in the PP..

Table 11: Mapping Between SARs and Assurance Measures

Assurance Measures	Security Assurance Requirements												
	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1[10]	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVE_VLA.1
Cisco PIX Firewall 520 Version 4.3(1) Installation and Configuration Document, Version 1.0			x				x						
Configuration Guide for the PIX 4.2				x			x						
Cisco PIX Firewall 520 Version 4.3(1) Administrative Guide White Paper, Version 1.0				x			x					x	
NT Workstation Architecture Document, Version 1.0				x	x								
PIX V4.3.1 Architecture and Detailed Design, Version 1.2				x	x								
PIX Firewall Syslog Server Document, Version 2.0				x	x								
System Log Messages for the PIX Firewall, Version 4.2				x	x								
PIX Firewall Series Version 4.1, Release Notes, Final							x						
PIX Firewall Quick Installation Guide 4.2				x			x						
Cisco PIX Target of Evaluation Test Procedures Document, Version 1.0									x	x	x		
TTAP PIX Firewall Vulnerability Assessment, Version 1.0													x
Configuration Management and Delivery Document, Version 1.0	x	x											
Hardware Functional Specification (Lego), Revision 1.2	x			x									
Cisco PIX Firewall 520 Version 4.3(1) Correspondence White Paper, Version 1.0						x							

[10] The only users of the TOE are administrative users. This SAR is not applicable to the TOE.

7 PP CLAIMS

120 This section provides the PP conformance claim statements.

7.1 PP Reference

121 The TOE conforms to the U.S. Government Traffic Filter Firewall Protection Profile for Low-Risk Environments, Version 1.c, November 1998.

7.2 PP Tailoring

122 The following PP functional requirements were further qualified for this Security Target:

• FIA_ATD.1	User attribute definition
• FDP_IFF.1	Simple security attributes
• FMT_MOF.1	Management of security functions behavior

7.3 PP Additions

123 The following security objectives for the environment were added in this ST: O.PHYSEC, O.GENPUR, and O.DIRECT.

8 RATIONALE

8.1 Security Objectives Rationale

124 This ST does not add additional TOE security objectives or threats to those identified within the TFFPP, Section 3.2.2 and 4.1, respectively. However, not all SFRs within the TFFPP are applicable to the TOE. This caused the T.REPEAT and T.PROCOM threats and O.SINUSE, O.ENCRYPT, and O.LIMEXT security objectives to not be applicable to the TOE.

125 The relationship of TOE threats to IT security objectives has been provided in Table 12. The grayed-out columns in Table 12 identify those threats and objectives that are not applicable to the TOE. The TOE security objectives' rationale is provided within Section 6.1 of the TFFPP.

Table 12: Mapping Between Threats and IT Security Objectives

	T.NOAUTH	**T.REPEAT**	**T.REPLAY**	**T.ASPOOF**	**T.MEDIAT**	**T.OLDINF**	**T.PROCOM**	**T.AUDACC**	**T.SELPRO**	**T.AUDFUL**
O.IDAUTH	X									
O.SINUSE		X	X							
O.MEDIAT				X	X	X				
O.SECSTA	X								X	
O.ENCRYP	X						X			
O.SELPRO									X	X
O.AUDREC								X		
O.ACCOUN								X		
O.SECFUN	X		X							X
O.LIMEXT	X									

126 The relationship of assumptions not completely met by the TOE to the additional security objectives for the environment is provided in Table 13.

Table 13: Mapping between Assumptions and Environmental Security Objectives

	T. PHYSEC	**T.GENPUR**	**T.DIRECT**
O.PHYSEC	**X**		
O.GENPUR		**X**	
O.DIRECT			**X**

127 O.PHYSEC is required to satisfy the assumption T.PHYSEC.

128 O.GENPUR is required to satisfy the assumption T.GENPUR.

129 O.DIRECT is required to satisfy the assumption T.DIRECT.

130 The rationale for threats not completely countered by the TOE and mapping to security objectives of the environment is presented in Section 6.2 of the TFFPP.

8.2 Security Requirements Rationale

131 The ST does not present additional security requirements defined within the TFFPP. The rationale for not satisfying all dependencies is given in Section 6.5 of the TFFPP.

132 The security requirements FIA_ATD.1, FDP_IFF.1, and FMT_ MOF.1 were legally tailored. The assignments preserved spirit and intent of the requirements.

133 The claim for password strength of function is consistent with the security objective, O.IDAUTH.

134 Since the spirit and intent of the TFFPP requirements has been maintained within this ST, as shown in Table 14, the set of security requirements (TOE and environment) are suitable to meet and are traceable to the security objectives.

135 The grayed-out columns in Table 14 identify those SFRs and security objectives that are not applicable to the TOE. Section 6.4 of the TFFPP justifies that the TOE SARs are appropriate.

Table 14: Mapping Between Security Objectives and SFRs

Security Objectives	Functional Security Requirements																			
	FMT_SMR.1	FIA_ATD.1	FIA_UID.2	FIA-AFL.1	FIA_UAU.1	FIA_UAU.4	FDP_IFC.1	FDP_IFF.1	FMT_MSA.3	FDP_RIP.2	FCS_COP.1	FPT_RVM.1	FPT_SEP.1	FPT_SMT.1	FAU_GEN.1	FAU_SAR.1	FAU_SAR.3	FAU_STG.1	FAU_STG.4	FMT_MOF.1
O.IDAUTH		x	x	▨	x	▨					▨									
O.SINUSE	▨	x	▨	▨	x	x	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
O.MEDIAT				▨		▨	x	x	x	x	▨									
O.SECSTA				▨		▨			x		▨									x
O.ENCRYP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	x	▨	▨	▨	▨	▨	▨	▨	▨	▨
O.SELPRO				x		▨					▨	x	x					x	x	
O.AUDREC				▨		▨					▨			x	x	x	x			
O.ACCOUN			x	▨		▨					▨				x					
O.SECFUN	x			▨		▨			x		▨							x	x	x
O.LIMEXT	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	x

8.3 TOE Summary Specification Rationale

136 The combination of the TOE Security Functions work together to satisfy the TSF as shown in Table 10. All security requirements map to security functions within the TOE. The absence of any security function invalidates the claim that the TOE satisfies the ST. The TOE Summary Specification, Section 6.1, describes the security functions of the TOE and how they satisfy the SFRs identified in Table 10.

137 The only security mechanism that is realized by a probabilistic or permutational implementation is the password generation mechanism. By requiring passwords to consist of 8 symbols from a 74-symbol list, with change frequency of at least once a year, the claim exceeds the strength of function requirement.

138 The TOE security assurance measures are exclusively based on the deliverables required by EAL2 as described in Section 6.2, Assurance Measures. These

deliverables are mapped to SARs in Table 11, to demonstrate that all TOE SARS are satisfied.

8.4 PP Claims Rationale

139 This ST does not include the following O.SINUSE, O.ENCRYPT, and O.LIMEXT security objectives described in the TFFPP because the TOE does not support the optional capabilities: remote administration and access to the TOE by authorized external IT entities. The absence of these security objectives means that the following optional requirements were also not included in this ST: FIA_AFL.1, FIA_UAU.4, and FCS_COP.1.